White Paper

radisys®

Diameter and LTE Evolved Packet System

By: Naveen Kottapalli, Lead Engineer

Overview

The popularity of always-on, IP-based services like YouTube, Twitter and Facebook is driving significant investment in network rollouts both for high capacity fixed line fiber-based networks and next generation mobile networks such as Long Term Evolution (LTE). All of these networks require secure and efficient provision of Authentication Authorization and Accounting (AAA) services, which forms the backbone of service administration including the mechanism to decide what services a user can access, at what Quality of Service (QoS) and how much to bill them.

Across the board, Diameter has been chosen as the AAA protocol in all next generation fixed and mobile IP-based networks. Diameter possesses significant advantages over legacy AAA solutions and is a cornerstone of the Evolved Packet System (EPS), which is the new core network supporting LTE. This paper discusses the Diameter Base Protocol in a holistic view and presents the reasons why Diameter is the preferred protocol for AAA services in these next generation networks.

CONTENTS

History of Diameter Base Protocol | Scalability | Fault-Tolerance *pg. 2*

Support of Agents | Secured Communication, Reliable Transmission | Capability Negotiation *pg. 3*

Load Balancing | Diameter Nodes Deployment | Diameter Node as a Client *pg. 4*

Diameter Node as a Server | Diameter Node as a Relay | Diameter Node as a Redirect | Diameter Node as a Proxy *pg. 5*

Diameter Node as a Translator | Diameter, the Choice of AAA in Evolving Networks *pg. 6*

The Role of Diameter in the EPS Architecture | Interface S6a *pg. 7*

Interface S6b | Interface S6c | Interface S6d Interface S9 | Interface S13 | Interface S13' | Interface Gx | Interface Gy | Interface Gz *pg. 8*

Interface Gi | Interface SGi | Interface Sp Interface Rx | Interface Rx+ | Interface Wm | How Has Diameter Replaced COPS? *pg. 9*

Is Diameter Only for Telecom Networks? Diameter as a Layer | Conclusion | Author *pg. 10*

History of Diameter Base Protocol

Before Diameter was defined by the Internet Engineering Task Force (IETF), there existed legacy access-control protocols including RADIUS (Remote Authentication Dial in User Service) and TACACS (Terminal Access Controller Access-Control System) that were, and continue to be, widely deployed. RADIUS has enjoyed significant deployment in most dial-up and initial broadband internet service provider (ISP) networks. However, the evolving and growing complexity of network architectures like IMS and EPS and the services expected to be delivered over those networks posed their own, higher demands on the AAA framework to provide stable, fault-tolerant and scalable protocols. These protocols needed to support the complex applications like Mobile-IP, Credit Control, NASREQ (Network Access Server Requirements), Billing Systems and so on.

Enter Diameter. The Authentication Authorization and Accounting (AAA) protocol, formally known as Diameter Base Protocol and mostly referred to as just "Diameter," is being widely used across all-IP (Internet Protocol) networks and in next generation telecom networks such as IMS (IP Multimedia Subsystem) and the EPS. Diameter (or "twice RADIUS") is evolved from the RADIUS protocol and was defined in an effort to overcome key limitations of RADIUS as listed here:

1. Limited scalability
2. No inherent network fault-tolerance
3. Lack of support of agents
4. Insufficient secured communication mechanisms
5. No support for reliable transmission
6. No ability to perform capability negotiation between nodes in the network
7. No support for network level load balancing

The following section further explores the impact each limitation has on the AAA network and how Diameter overcomes each limitation.

Scalability

One of the major drawbacks of the RADIUS protocol is the inability to scale itself when deployed in a network. The RADIUS protocol does not define any procedures that enable a node to crawl on the network to build its own operative RADIUS network.

The Diameter protocol overcomes this limitation by defining an optional* procedure to discover new nodes in the network using DNS (Domain Name System) services.

How Does the Scalability Limitation Impact Network Deployment?

Scalability is an important aspect of any protocol that enables any node to build its own network. If scalability is not defined, then the job of configuring all hosts and their addresses in a complex network is a nightmare job. It may also tempt administrators to reuse the shared key, which results in vulnerability– especially when the authenticator is not globally and temporally unique.

Fault-Tolerance

Another drawback of the RADIUS protocol is that there is no provision for provide fault-tolerance when it is deployed in a network. The RADIUS protocol does not define the procedures that enable a node to perform failover or failback on the network when any of the other node's services are not available.

The Diameter protocol overcomes this limitation by defining an optional* procedure to do failover or failback to one of the other connected nodes.

How Does the Fault-Tolerance Limitation Impact Network Deployment?

The fault-tolerance aspect enables any node to reach the final destination of the packet via one or more alternate paths. If this is not defined, then the node might become more vulnerable to its own failures or the failure of other elements in the AAA network and cannot guarantee message delivery.

Support of Agents

In addition to the other limitations above, the RADIUS protocol has no defined ways a RADIUS node can be deployed or its responsibilities defined—i.e., it doesn't clearly define the procedures of how a RADIUS node can work on the packets that it might receive, transmit and forward.

The Diameter protocol overcomes this limitation by defining the clear responsibilities of all possible Diameter node deployment modes—either as Proxy or Redirect or Relay or Translation Agents.

How Does the Support of Agents Limitation Impact Network Deployment?

This kind of feature enables network administrators to clearly segregate different nodes based on their responsibilities, which enables efficient load distribution and makes the job of maintaining the network easier.

Secured Communication

The RADIUS protocol lacks any definition of secure transport of messages.

The Diameter protocol overcomes this limitation by providing an optional secure transmission of Diameter packets.

How Does the Secured Communication Limitation Impact Applications?

Lack of embedding this feature in the protocol leaves the burden at the application layer. Having this feature at the protocol level leaves the application to take care of business logic instead of handling the responsibilities of the layers below.

Reliable Transmission

Another drawback of the RADIUS protocol is that it uses UDP (User Datagram Protocol) at its lower layer for transmission of the packets and doesn't define the procedures about retransmission of the packets in case of any failure.

The Diameter protocol overcomes this limitation by transmitting the Diameter packets over TCP (Transmission Control Protocol) or SCTP (Stream Control Transmission Protocol).

How Does the Reliable Transmission Limitation Impact Applications?

Lack of reliable transmission at the node level will impose more load at the application layer such as retransmission of messages, maintaining different timers for different kind of messages and so on.

Having this feature at the protocol level leaves the application to take care of business logic instead of handling the responsibilities of the layers below.

Capability Negotiation

Yet another drawback of RADIUS is the lack of procedures defining the exchange of capabilities with other RADIUS nodes, leaving peer nodes unaware of the applications that the other node is supporting.

Diameter overcomes this limitation by mandating the exchange of capabilities whenever a connection is established with any peer node.

How Does the Capability Negotiation Limitation Impact the Network?

Lack of capability negotiation at any node will impose a lot of burden upon configuration of peers. Having this feature in place at the protocol level will enable the nodes to know in advance about the peers—such as applications, security mechanisms, etc.—before starting the traffic.

Load Balancing

Another drawback of RADIUS is the lack of procedures defining load balancing among various nodes with which it can communicate.

Diameter overcomes this limitation by defining the load balancing capability among the connected peers by designating the peers as primary or secondary.

How Does the Load Balancing Limitation Impact the Network?

Lack of load balancing at any node will impose a lot of burden on one particular node to process the traffic that is coming from various connected nodes. This also compels the operator to have more advanced hardware to process the traffic.

Diameter Nodes Deployment

Diameter nodes in a network deployment will look like a chain of nodes linked together, each defined with respective roles and responsibilities. A typical node deployment looks as follows.

A Diameter node can be deployed as one or more of the following types:

1. Client
2. Server
3. Relay
4. Redirect
5. Proxy
6. Translator

Each of the node types is bounded with clear responsibilities which make the development and deployment easy, each sharing the following common properties:

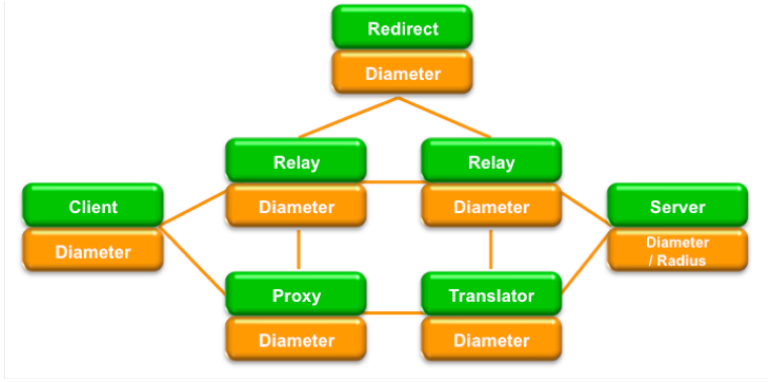

Figure 1.

1. Has the Diameter Base Protocol.
2. Will have either TCP or SCTP at its lower layer.
3. Shall produce or validate the TLS (Transport Layer Security) certificates provided by other nodes.

Let us look more closely at what each node type does.

Diameter Node as a Client

A Diameter node which is placed at the edge of a network that performs access control, such as Non Access Stratum (NAS) or FA (Foreign Agent), will be named as a client and has the following properties:

1. Sends connection/association requests to servers.
2. Occasionally discovers a first hop agent.
3. Invokes failover or failback procedures whenever required.
4. Hosts an AAA application which generates the requests and expects the responses.
5. May maintain either state-full/or state-less Authorization State Machines.
6. May maintain either state-full/or state-less Accounting State Machines.
7. May maintain non-volatile memory for safe storage over network failures.

Diameter Node as a Server

A Diameter node which performs the authentication and/or authorization of users will be named as a server and has the following properties:

1. Accepts connection/association requests from clients.
2. Occasionally may initiate messages.
3. Performs loop detection and duplicate detection on received messages.
4. Performs authentication and/or authorization and/or accounting upon received requests.
5. May re-authenticate, re-authorize or abort the established sessions.
6. Maintains either state-full/or state-less Authorization State Machines.
7. Maintains either state-full/or state-less Accounting State Machines.
8. Cleans the sessions whenever required, like session time out, client restart, etc.

Note: A Diameter node can be deployed as both client and server; this will usually be the case when the node is acting as an intermediate node between any two Diameter nodes. For example, a Diameter node acting as Relay will have both the properties of client and server.

Diameter Node as a Relay

A Diameter node which is placed in the message forwarding path will be named as a relay and has the following properties:

1. Accepts connection/association requests from clients and sends connection/association requests to servers.
2. Will append Route-Record to all requests forwarded.
3. Will never originate any AAA messages.
4. Will never validate the semantics of messages.
5. Finds a suitable upstream server for forwarding the messages based on information in routing Attribute-Value Pairs (AVPs) and realm information.
6. Performs loop detection on received messages.
7. Does not keep track of session or resource states.

Diameter Node as a Redirect

A Diameter node which facilitates the other nodes to establish the connection with a requested node directly will be named as a redirect and has the following properties:

1. Accepts connection/association requests from clients.
2. Will not be placed in the message forwarding path and refers the Diameter clients to Diameter servers.
3. Will neither originate nor alter AAA messages.
4. Will never validate the semantics of messages.
5. Does not keep track of the session or resource states.

Diameter Node as a Proxy

A Diameter node which may enforce the policies as part of forwarding messages will be named as a proxy and has the following properties:

1. Accepts connection/association requests from clients and sends connection/association requests to servers.
2. Shall be placed in the message forwarding path and shall append Route-Record to all requests forwarded.
3. May originate any AAA reject messages for the received request from client.
4. Validates the semantics of AAA messages.
5. Shall keep track of the NAS resources and make policy decisions. As part of policy enforcement, messages shall be modified.
6. Finds a suitable upstream server for forwarding the messages.
7. Performs loop detection on received messages.

Diameter Node as a Translator

A node which acts as a translator between a Diameter node and a RADIUS node will be named as a translation agent and has the following properties:

1. Accepts connection/association requests from clients and sends connection/association requests to servers.
2. Translates the messages of type RADIUS/TACACS to Diameter and Diameter to RADIUS/TACACS.
3. Will validate the semantics of AAA messages.
4. Will maintain the session and transaction states for long-lived authorized sessions.

Diameter, the Choice of AAA in Evolving Networks

There are a few requirements to be met by any AAA protocol to be suitable for evolving networks. The following section explores how Diameter satisfies the major general AAA criteria to become an integral part of evolving networks.

1. Scalability—Diameter is capable of handling thousands of simultaneous transactions expanding its capabilities with the help of the Peer Discovery feature.
2. Failover—Diameter is capable of changing the service to a backup server when the primary server is down.
3. Mutual auth AAA Client/Server—Diameter is capable of supporting the mutual authentication between AAA clients and servers with the help of the messages that are defined.
4. Transport Level Security—Diameter provides authentication, integration protection and confidentiality at the transport layer with the help of TLS; Diameter uses this feature to make all AAA transactions secure between peers.
5. Data Object Confidentiality—Diameter provides flexibility to encrypt the AVPs embedded inside the message, which can then be decrypted by the target AAA entity.
6. Data Object Integrity—Diameter provides the chain of authenticated proxies or brokers throughout the AAA message traversal to the target entity.
7. Certificate transport—Diameter is capable of transporting certificates in lieu of requiring that an out-of-band protocol be used to fetch certificates.
8. Reliable AAA transport—Diameter is sufficiently resilient against packet loss including Hop-by-Hop retransmission, failover, retransmission and timely delivery of AAA responses.
9. Support of IPv4 and IPv6—Diameter is capable of running over both IPv4 and IPv6.
10. Support of Proxy and Routing Brokers—Diameter supports the presence of Proxy or Redirect agents in the message forwarding path.
11. Convergence—Diameter supports the presence of translation agents, through which it provides interoperable with legacy protocols like RADIUS.

The Role of Diameter in the EPS Architecture

Diameter has been chosen for evolving networks not just for meeting the above-mentioned criteria, but also for providing transfer of Quality of Service (QoS) as well as bandwidth and rating policies. The presence of Diameter in the EPS is spread across various interfaces and not simply limited to those shown in Figure 2.

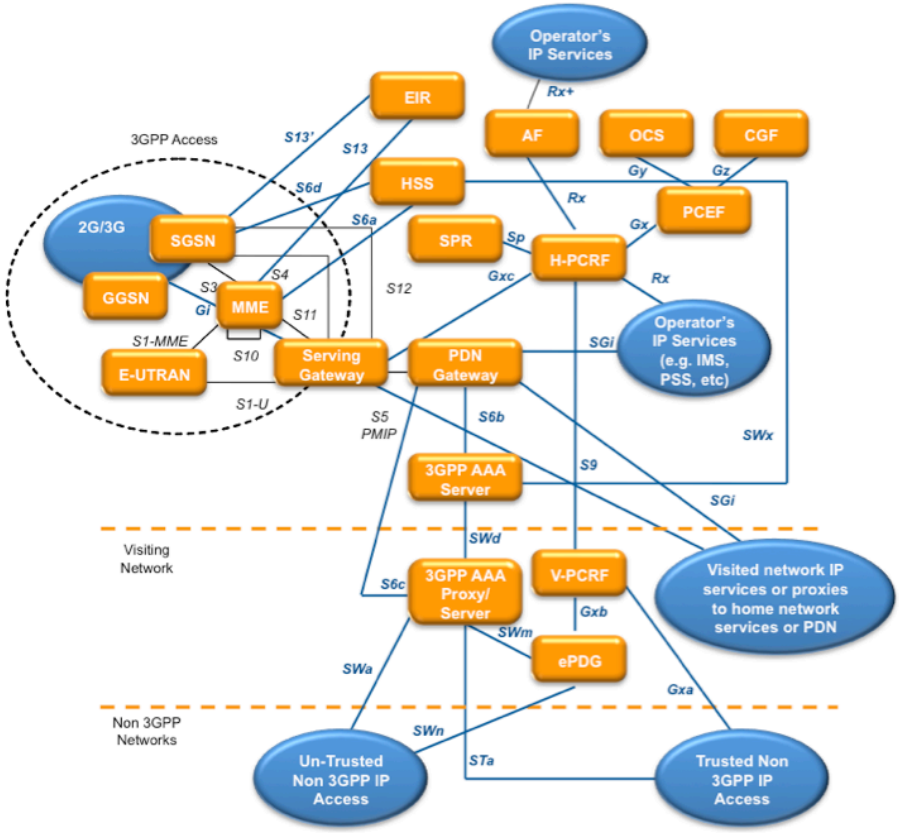

Figure 2.

Interface S6a

The interface S6a lies between the HSS (Home Subscriber Server) and the MME (Mobility Management Entity) for authentication and authorization. This interface has the following properties:

1. Transport of subscriber related data.
2. Transport of location information.
3. Authorizing a user to grant access to EPS.
4. Transport of authentication information.

Interface S6b

The reference point S6b lies between the PDG (PDN Gateway) and the 3GPP AAA Proxy/Server for mobility-related authentication. This interface has the following properties:

1. Transport of commands to retrieve and store the mobility parameters.
2. Transport of static QoS.

Interface S6c

The reference point S6c lies between the PDG in the HPLMN (Home Public Land Mobile Network) and the 3GPP AAA Server for mobility-related authentication. This interface has the following property:

1. Transport of commands to retrieve and store the mobility parameters.

Interface S6d

The interface S6d lies between the HSS and the SGSN (Serving GPRS Support Node) used to retrieve and store mobility-related parameters. This interface shares the same properties as those of S6a.

Interface S9

The reference point S9 lies between the H-PCRF (Home Network-Policy Charging and Rules Function) and the V-PCRF (Visited Network-Policy Charging and Rules Function) in the EPS network. This interface has the following properties that enable the H-PCRF:

1. Dynamic PCC control, including both PCEF and, if applicable, BBERF (Bearer Binding and Event Reporting Function) in the VPLMN.
2. Transport of IP-CAN-specific parameters from both the PCEF and, if applicable, the BBERF in the VPLMN.
3. Serves Rx authorizations and event subscriptions from the AF in the VPLMN.

Interface S13

The reference point S13 lies between the MME and the EIR (Equipment Identity Register). This interface has the following property:

1. Enables the ME Identity check procedure between the MME and the EIR.

Interface S13'

The reference point S13' lies between the SGSN and the EIR and has the similar property as that of S13.

Interface Gx

The reference point Gx lies between the PCRF (Policy Charging and Rules Function) and the PCEF (Policy Control Enforcement Function) in the EPS network and enables the PCRF to have dynamic control over PCC behavior at the PCEF. This interface has the following properties:

1. Enables the signaling of PCC decisions.
2. Negotiation of IP-CAN bearer establishment mode.
3. Termination of Gx session.

Interface Gy

The online charging reference point Gy lies between the PCEF and the OCS (Online Charging Function). This reference point Gy provides the same functionalities as those of reference point Ro.

Interface Gz

The offline charging reference point Gz lies between the PCEF and the CGF. This reference point Gz provides the same functionalities as those of Rf in the EPS.

Interface Gi

The reference point Gi lies between the Packet Domain and the external PDN (Packet Data Network). As an example, Gi lies between the GGSN and external IP networks. This reference point Gi provides the following functionalities:

1. Transfer of authentication and authorization information during Access Point Name (APN) provisioning.
2. Transfer of accounting information during APN provisioning.

Interface SGi

The reference point SGi lies between the EPC-based PLMN and external PDN. As an example, SGi lies between the PGW and external IP networks. This reference point SGi provides similar functionality to that of the Gi interface.

Interface Sp

The reference point Sp lies between the SPR (Subscription Profile Registry) and the PCRF (Policy Control and Charging Rules Function). This reference point provides following functionalities and is not limited to:

1. Transfer of subscriber information related to IP-CAN based on subscriber Id.
2. Unsolicited notifications about subscriber information change

Interface Rx

The reference point Rx lies between the AF and PCRF. This reference point provides the transport of application-level session information and is not limited to:

1. IP filter information that identifies service data flow for the policy control.
2. QoS control of media/application bandwidth.
3. Notifications on IP-CAN bearer level events.

Interface Rx+

The reference point Rx+ is the Rx reference point for the EPC. This reference point lies between the PCRF and IP services or proxies to network services. This reference point provides the transport of application-level session information similar to Rx.

Interface Wm

The intra-operator reference point Wm lies between the PDG and a 3GPP AAA Proxy/Server. This interface has the following properties:

1. Applies for WLAN 3GPP IP access.
2. Transport of tunneling attributes and WLAN UE's IP configuration parameters.
3. Transport of charging data for 3GPP PS-based service charging.
4. Transport of user authentication and authorization data.

Along with the above-mentioned interfaces, Diameter is being used in evolving networks like IMS, 3GPP networks, and other non-3GPP networks too. Some of these interfaces include Cx, Dx, Sh, Dh, Zh, Dz, Zn, Zn', Dw, Wa, Wd, Wx, Wg, Gmb, Mz, Tx, Ty, Re, SWa, SWn, SWm, SWx, H2, E2, E4, E5, Re, A3, A4, Rw, Rs...

How Has Diameter Replaced COPS?

COPS (Common Open Policy Service) was initially selected by 3GPP for the transfer of policy information between PDPs (Policy Decision Points) and PEPs (Policy Enforcement Points) of IMS in the initial release (Release 5) of the specifications. In later releases of IMS specifications, 3GPP decided to replace COPS with Diameter because of the following:

1. More scalable protocol
2. More robust protocol with built-in failover procedures defined.
3. Support of agents.
4. Capability negotiation with immediate nodes.

Is Diameter Only for Telecom Networks?

With the expanding territory of Diameter in evolving networks, the protocol is finding its own way beyond the AAA space, and not only in the telecom domain: it has also become a favorite protocol for any IP-based application that requires AAA. The following diagram depicts the usage of Diameter between two IP applications.

These IP applications can range from authentication servers to billing servers. The flexible architecture of Diameter enables the vendors to define their own specific commands with their own AVPs (if the vendor doesn't need interoperability).

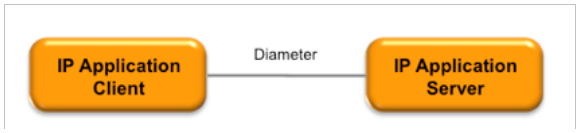

Figure 3.

Diameter as a Layer

Diameter sits above the transport layer when it is viewed in the OSI (Opens Systems Interconnection) layered architecture. It uses the transport services provided by either TCP or SCTP layers, which in turn use IP as their layer below as illustrated in Figure 4.

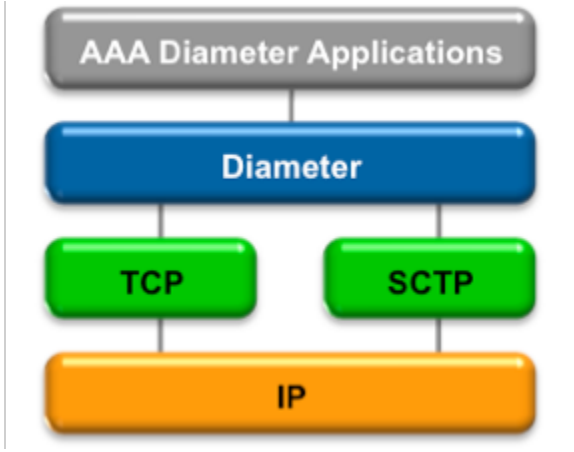

Figure 4.

Conclusion

As described at the top of the paper, the popularity of always-on, IP-based (generally internet) services like is driving significant investment in network rollouts. Each of these networks requires secure and efficient provision of AAA services, which forms the backbone of service administration. Across the board, Diameter has been chosen as the AAA protocol in all next generation fixed and mobile IP-based networks because it possesses significant advantages over legacy AAA solutions and is thus a cornerstone of the EPS, the new core network supporting LTE.

Author

Naveen Kottapalli, Lead Engineer

radisys.

Corporate Headquarters
5435 NE Dawson Creek Drive
Hillsboro, OR 97124 USA
503-615-1100 | Fax 503-615-1121
Toll-Free: 800-950-0044
www.radisys.com | info@radisys.com

intel Embedded Alliance Premier